



Department of Homeland Security Daily Open Source Infrastructure Report for 14 April 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports a chemical smell — possibly pepper spray — sickened several people and forced the evacuation of a terminal at Sacramento International Airport on Wednesday, April 12. (See item [21](#))
- The Associated Press reports health officials have said that two infected airline passengers may have helped spread Iowa's mumps epidemic to six other Midwestern states. (See item [30](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *April 13, Associated Press* — **Small fire closes University of Connecticut power plant.** The University of Connecticut's power plant was closed Thursday morning, April 13, after a fuel leak caused a fire near one of the turbines. No injuries were reported. The small fire occurred shortly after 10 a.m. EST in the Glenbrook Road facility. A fuel-line fitting came loose and diesel fuel spilled, catching on fire near one of three large turbines that recapture heat produced by the plant, said University spokesperson Richard Veilleux. The building's fire-suppression system extinguished the flames before they could spread, and the damage did not appear to be serious, he said. Two adjacent buildings were evacuated. The university switched from its own power to the Connecticut Light and Power grid while the fire was being investigated.

Source: http://www.boston.com/news/local/connecticut/articles/2006/04/13/small_fire_closes_uconn_power_plant/?rss_id=Boston.com+%2F+News

2. *April 12, KRIS TV 6 News (TX)* — **Fourth man pleads guilty in electric grid fraud case.** A former senior manager with the organization that runs Texas' electricity grid pleaded guilty to organized crime and theft charges and agreed to repay \$500,000 he pocketed in an elaborate scheme. Chris Douglas faces up to nine years in prison, Texas Attorney General Greg Abbott said. Douglas and five others were charged in January 2005 with devising a scheme inside the Electric Reliability Council of Texas, known as ERCOT, in which they allegedly created bogus companies that charged more than \$2 million for fake work done by nonexistent employees and even a dead person.

Source: <http://www.kristv.com/global/story.asp?s=4762501>

3. *April 12, Associated Press* — **Utility sues Union Pacific, claiming scheme to hold back coal.** Entergy Arkansas claims Union Pacific Railroad schemed to hold back deliveries of Wyoming coal to Arkansas power plants in an effort to make more money. In a suit filed Tuesday, April 11, Entergy claimed that the railroad "in a conscious and deliberate practice" limited supplies of coal from the Powder River Basin in Wyoming in an effort to manipulate demand and ultimately maximize its profits. Entergy Arkansas said that it suffered "tens of millions of dollars" in damages when coal shipments declined up to 20 percent last year. The company said the coal shortage forced it to reduce operations at two large coal-fired power plants in Arkansas, the White Bluff plant near Redfield, and the Newark plant in Independence County. The electric utility said the production cutbacks forced it to increase purchases on the open market, at greater cost. Union Pacific says bad conditions — including a snowstorm and two derailments last May — warped rail lines near the region where the coal shipments originate. The coal dispute is a factor in a state Public Service Commission investigation of a recent electricity rate increase by Entergy's, and another increase planned for April that was suspended.

Source: <http://www.casperstartribune.net/articles/2006/04/12/news/wyoming/fe57eb99599a88198725714e005977c3.txt>

4. *April 12, BBC* — **Chevron invests in India refinery; company looking to increase presence in Asia.** U.S. oil giant Chevron is investing \$300 million in a new Indian refinery as it looks to meet growing demand from Asia. It is buying five percent of Reliance Petroleum. The 580,000 barrels-per-day site in Jamnagar will process heavy crude and is due to open in December 2008. It will sit next to another similar sized Reliant-owned facility, creating the world's biggest refinery complex. Chevron has an agreement with Reliance to try to collaborate on other energy projects in the region. "This underscores the importance of Asia to Chevron generally, and India specifically," said Chevron chief executive Dave O'Reilly. Chevron said the new refinery would increase its ability to process a wide variety of hard-to-refine crude oils.

Source: <http://news.bbc.co.uk/1/hi/business/4904142.stm>

5. *April 12, Reuters* — **International Energy Agency raises estimate of need for OPEC oil in 2006.** The Organization of the Petroleum Exporting Countries (OPEC) will need to pump more oil this year than previously expected to meet rising world demand and cover a shortfall from other producers such as Russia, the International Energy Agency (IEA) said on Wednesday,

April 12. The agency also said it expected no early end to concerns over Iranian supply, raised by Tehran's nuclear row with the West, and lost output in Nigeria that have helped push oil near a record high this week. The IEA's report points to a narrower balance between supply and demand, analysts said. Higher-than-expected use in the Middle East and Asia Pacific prompted IEA to raise its estimate for world demand this year by 300,000 barrels per day to 85.1 million bpd. While raising demand figures, the IEA trimmed its estimate for growth in oil use in 2006 by 20,000 bpd to 1.47 million bpd and said demand would be higher with lower oil costs.

Source: http://news.yahoo.com/s/nm/20060412/bs_nm/energy_iea_dc_3

6. *April 12, Associated Press* — **Three companies in pipeline partnership.** PG&E Corp., Williams Cos., and Fort Chicago Energy Partners LP will create a new partnership — Pacific Connector Gas Pipeline LP — to build a previously announced proposed pipeline project. The proposed 223-mile would increase West Coast access to natural gas supplies starting in 2010. It would connect to the proposed Jordan Cove liquefied natural gas terminal near Coos Bay, OR, link up with the Northwest Pipeline near Roseburg, OR, and tie in near the California-Oregon border to PG&E's gas transmission system. The proposed pipeline would deliver up to one billion cubic feet per day of natural gas to the West Coast. A Federal Energy Regulatory Commission certification application is to be submitted in January 2007, with construction planned for summer 2009.

Source: http://biz.yahoo.com/ap/060412/pg_e_agreement.html?v=1

7. *April 12, Orlando Sentinel (FL)* — **Utility gears up to prepare for hurricanes and more.** The Kissimmee Utility Authority (KUA) conducted a full-scale disaster exercise on Thursday, April 13 to assess the agency's emergency preparedness. The four-hour drill was to involve a wide range of activities, including both live-action training and tabletop exercises. Activities were to include pre- and post-hurricane scenarios as well as a series of exercises to gauge how effectively the utility would respond to a pandemic or other major health threat, such as avian influenza. "In a pandemic, essential services such as power and water could be disrupted, and crucial workers sickened or killed...We have a responsibility to keep the power flowing, no matter what the disaster might be," said Jef Gray of KUA.

Source: http://www.orlandosentinel.com/news/local/osceola/orl-owgovw_atch12_106apr12.0.73822.story?coll=orl-news-headlines-osceola

8. *April 11, Associated Press* — **India hopes for \$7 billion from oil investments.** India expects to earn more than \$7 billion when it awards 55 new oil and natural gas exploration fields to successful bidders over the next two years, said Murli Deora, India's petroleum minister, on Tuesday, April 11. Meanwhile, India is on schedule to start production of coal-bed methane gas by 2007, petroleum secretary M.S. Srinivasan, said. In the latest round of bidding, onshore oil exploratory blocks are being offered in 11 states, mostly in central and northeastern India. The offshore blocks being offered are located off the country's western and eastern coasts and the Andaman islands in the Indian Ocean. Ten coal-bed methane fields are being offered for exploration in the states of Andhra Pradesh, Chattisgarh, Madhya Pradesh, Rajasthan, Jharkhand and West Bengal. India has so far awarded 110 fields through an international competitive bidding process to boost the country's oil and gas production. A series of gas discoveries along the Indian coast in recent years, combined with the opening of the Indian market to supplies from outside, have fueled prospects for increasing gas consumption in the

country.

Source: <http://www.chron.com/disp/story.mpl/ap/fn/3786515.html>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

9. *April 12, Reuters* — **Defense stocks may jump higher with big profits.** Shares of U.S. defense companies, which have nearly trebled since the beginning of the occupation of Iraq, show no signs of slowing down as investors anticipate strong first-quarter profits this month. U.S. defense spending is rising faster than expected — confounding experts who predicted a slowdown — and rumors of cuts to big programs have not turned into reality. Allied with a boom in commercial aerospace, the profit outlook for defense contractors has never looked more robust.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/04/12/AR2006041201540.html>

10. *April 12, Defense News* — **U.S. metal shortages hinder Army aircraft in Iraq.** Shortages in U.S. stocks of specialty metals are leading to critical spare parts shortages for Army helicopters flying in Iraq. Spare parts manufacturers are unduly constrained by the Berry Amendment and it is causing critical shortages in the specialty steel that goes into bearings used in helicopters, said Major General James Pillsbury, commander of the Army's Aviation and Missile Command. Pillsbury said shortages in U.S. stocks of other specialty metals, such as titanium, are also leading to supply chain backups.

Source: <http://www.defensenews.com/story.php?F=1683910&C=america>

[\[Return to top\]](#)

Banking and Finance Sector

11. *April 12, Reuters* — **Ross-Simons says security breach exposes customers.** Ross-Simons, which sells specialty merchandise through retail stores and more than 60 million catalogs each year, on Tuesday, April 11, said a security breach could allow unauthorized access to its customers' confidential financial information. Although the security snafu has been identified and corrected and the matter is under investigation, Ross-Simons said it may have exposed private-label credit card numbers and other personal information of those who had applied for the cards.

Source: <http://www.computerworld.com/securitytopics/security/story/0.10801.110425.00.html>

12. *April 12, TechWeb* — **E-filing tax season draws out hijackers, pharmerers, scammers.** A

security company employee is warning taxpayers that their personal information can be vulnerable even if they type and enter the Internal Revenue Service's (IRS) Website address. In addition to sending suspicious e-mails, scammers could also try hijacking and rerouting legitimate Web queries' to steal taxpayers' identities, according to CDW system engineer G. Thomas Vanek. Vanek said hackers can intercept a legitimate request as it travels over the Ethernet to seamlessly reroute the request to a fake, but nearly identical site. With the amount of phishing related to IRS scams Vaneck said other types of hacking are probably underway. "The IRS hasn't come out and issued any verbage about pharming, but I have no doubt it's being attempted," he said. That's partly because protocols haven't been updated in 30 years, Vanek said.

Source: <http://www.techweb.com/wire/security/185300923;jsessionid=XHQLWPFCJMYJSQSNDDBCSKHSCJUMEKJVN>

13. *April 12, Press-Register (AL)* — **Nigerian gets more than three years for bank scam.** A federal judge in Mobile, AL sentenced a Nigerian man to almost three and a half years in prison Tuesday, April 11, punishing the defendant in a two-state bank fraud involving stolen corporate bank checks. Oluyomi Oshinaike recruited people in the Mobile area to allow their bank accounts to be used to deposit money from a pair of bogus checks. The checks had been intercepted by a postal worker at a postal facility in Georgia and then altered. Oshinaike was charged with depositing two checks totaling more than \$227,000 into the bank accounts of a woman he met at an Atlanta nightclub and that woman's mother. He was part of an operation that federal prosecutors in Atlanta said involved between \$1 million and \$2.5 million in altered checks. After Tuesday's hearing, Assistant U.S. Attorney E.T. Rolison described the operation as a classic Nigerian scam. Like e-mail solicitations many have received, Rolison said, Oshinaike and others used various cover stories to persuade people to cooperate. One version involved a wealthy father in Nigeria who needed help getting money out of the African nation, he said.

Source: http://www.al.com/printer/printer.ssf?/base/news/11448337042_76160.xml&coll=3

14. *April 12, InformationWeek* — **Web application hack incidents increase.** Website hacks are on the rise and pose a greater threat than the broad-based network attacks faced by IT departments. Attacks against Web applications threaten to steal critical customer, employee, and business partner information stored in applications and databases linked to the Web. Web hacking attacks numbered 58 in 2005, up from 16 in 2004 and nine in 2003, according to the Web Application Security Consortium. Another 20 attacks have been reported this year against sites including Sourceforge.net and MySpace.com, putting 2006 on pace to be the worst year yet. This trend is particularly disturbing to financial services companies. Bank of America reported on Tuesday, April 11, that sales of products via the bank's Website totaled 3.8 million accounts in 2005, an increase of 69 percent over the previous year. This included 2.3 million online activations, 380,000 new savings accounts, 375,000 new credit card accounts, and 298,000 new checking accounts. A TD Canada Trust survey of more than 700 consumers found that less than 30 percent of Web banking users were aware of the terms "phishing" and "Website spoofing." Most customers believe their bank should be primarily responsible for security measures regarding online banking.

Source: <http://www.informationweek.com/showArticle.jhtml;jsessionid=IMOESPOBG2TZQOSNDBECKICJUMEKJVN?articleID=185300842>

15. *April 12, Associated Press* — **Federal charges tie temp agencies to money laundering.** Two temporary employment agencies and nine of their employees are accused in federal charges of sending illegal immigrants with false documentation to Ohio businesses seeking temporary workers, while scamming millions of dollars in fees from those businesses. The case illustrates the government's effort to link job agencies that illegally supply illegal alien workers to money laundering, Dean Boyd, a spokesperson for the Department of Homeland Security's Immigration and Customs Enforcement Agency, said Wednesday, April 12. Federal agents arrested three people in Philadelphia, one in New York City and another in Columbus, OH. The government accused the agencies, identified as HV Connect and TN Job Service, of a \$5.3 million money–laundering scheme. The agencies would place workers they said had U.S. work authorization and promise to pay payroll taxes and workers' compensation premiums from fees paid by the employers. The government accuses the agency workers of using the money instead to build a home, buy jewelry and liquor, and spend money at casinos. The undocumented workers were paid in cash.

Source: <http://www.phillyburbs.com/pb-dyn/news/104-04122006-640536.h tml>

16. *April 12, Sophos* — **Prague phishing stooge arrested by police.** SophosLabs reports that Czech authorities have arrested a man suspected of involvement in a gang which phished the bank accounts of innocent Internet users. In what is said to be the first arrest of its kind in the Czech Republic, a man was arrested while waiting at a bank counter in Prague, where he was said to have been attempting to pick up money stolen through the phishing scheme. If found guilty, the man faces up to 12 years in prison. According to the police, the detained man was hired by a criminal gang to withdraw money from a bank account, which had had funds transferred to it from plundered accounts belonging to Citibank customers. The gang is said to have sent a number of e–mails disguised as communications from Citibank, asking for recipients to confirm their bank account details and other personal data.

Source: <http://www.sophos.com/pressoffice/news/articles/2006/04/czec hphish.html>

17. *April 11, Computerworld* — **Update: Florida residents' data exposure a statewide issue.** The Social Security numbers, driver's license information, and bank account details belonging to potentially millions of current and former residents of Florida are available to anyone on the Internet because sensitive information has not been redacted from public records being posted on county Websites. Although questions about the availability of personal data online initially focused on Broward County, all counties in Florida are subject to the same state law. According to Sue Baldwin of the Broward County Records Division, counties across the nation face the same issue. She noted that the information on the Web is in full compliance with state statutes that require counties to post public documents on the Internet. Bruce Hogman, a county resident who raised concerns about the availability of information with the Broward County Records Division, said it poses a serious risk of identity theft and fraud. The exposure stems from the county's failure to remove sensitive data from images of public documents such as property records and family court documents. Included in the documents publicly available are dates of birth and Social Security numbers of minors, images of signatures, passport numbers, green–card details and bank account information.

Source: <http://www.computerworld.com/printthis/2006/0.4814.110389.00 .html>

[[Return to top](#)]

Transportation and Border Security Sector

18. *April 13, Associated Press* — **US Airways completes refinancing.** Air carrier US Airways Group Inc. on Wednesday, April 12, said it has completed a \$1.25 billion debt refinancing transaction. The loan is underwritten by GE Commercial Finance and Morgan Stanley Senior Funding. US Airways said it is using the debt refinancing to pay off four previous loans as well as for general corporate purposes.
Source: http://biz.yahoo.com/ap/060412/us_airways_group_loan.html?.v=1
19. *April 13, The Star-Ledger (NJ)* — **New Jersey Transit project to ease Manhattan traffic.** On Wednesday, April 12, New Jersey Transit approved a project intended to provide relief for harried rail commuters into Manhattan's bustling Penn Station. The project includes design work for a new concourse to connect with a new train station planned for the West Side of Manhattan. The new station, Moynihan Station, is considered a critical component of the \$6 billion Access to the Region's Core project that will expand capacity of the New York Penn Station complex. A new rail crossing under the Hudson River, the Trans-Hudson Express Tunnel, is part of the venture.
Source: <http://www.nj.com/news/ledger/jersey/index.ssf?/base/news-3/114491032643940.xml&coll=1>
20. *April 13, Insurance Journal* — **Truckers use new fatigue monitoring device.** Fatigue plays a role in 13 percent of all truck crashes, according to a March report by the Federal Motor Carrier Safety Administration, and the government estimates about 15,000 people are killed each year in fatigue-related accidents involving cars, trucks, or other motor vehicles. Now, some truckers are testing a new warning device that could help avoid disasters by tracking how often they blink and how long their eyes stay shut — if they would be willing to accept such monitoring, which an independent researcher questions. What may happen to the data, however, is a cause for concern for truckers. The device, designed by former Carnegie Mellon University professor Richard Grace, is about the size and shape of a Web cam. It is mounted on the dashboard, powered by the truck's cigarette lighter, and uses infrared technology to monitor blinking. As the driver's blinking increases — and the duration the driver's eyes are closed increases — the device beeps. It keeps beeping for each second the driver's eyes close, alerting the trucker that it's time to pull over. Grace said truckers don't like to wear monitoring devices and that his machine detects fatigue quicker than most lane-tracking devices.
Source: http://www.insurancejournal.com/news/national/2006/04/11/672_26.htm
21. *April 12, Associated Press* — **Chemical odor prompts evacuation at Sacramento airport.** A chemical smell that sickened several people forced the evacuation of a terminal at Sacramento International Airport on Wednesday, April 12. Hazardous materials teams responding to the 11:15 a.m. PDT incident concluded that a passenger might have released pepper spray in a part of the terminal that serves United and American airlines. Several people reported eye irritation and coughing, said Karen Doron, a spokesperson for the Sacramento County Airport System. About 200 people were evacuated from a wing of terminal B-1. Doron said several passengers told authorities they had attended a safety conference in Sacramento where the instructor handed out pepper spray, a small aerosol container that can be used for self defense.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/14327017.htm

22. *April 12, WUSA-TV (DC)* — **Amtrak service temporarily stopped from Washington, DC to Florida.** Amtrak said it was suspending service between Washington, DC and Florida on Wednesday, April 12, and Thursday, April 13, because of repairs being made to a bridge in North Carolina by CSX Corp., which owns the rail corridor. Amtrak is offering refunds and future travel dates for affected passengers.

Source: http://www.wusatv9.com/news/news_article.aspx?storyid=48395

23. *April 12, Sci-Tech Today* — **Virgin Atlantic leads way for radio frequency identification.** Virgin Atlantic is evaluating whether or not to extend the use of radio frequency identification (RFID) tagging to track plane parts, following a four-month trial of the technology. The airline has been using RFID to track high-value aircraft parts at its logistics center in Heathrow Airport near London since November, and says the results will help develop a business case for more widespread use. The airline is working with Airbus and other suppliers to see how they will integrate RFID into their logistics programs.

Source: http://www.sci-tech-today.com/story.xhtml?story_id=03000000R_HLU

24. *April 06, Transportation Security Administration* — **TSA trains police officers to spot terrorist related activity.** The Transportation Security Administration (TSA) has launched a campaign to ensure that state and local law enforcement officers throughout the U.S. are trained to detect potential terrorist-related activities in their communities and on their roadways. TSA has commissioned the Counterterrorism Division of the Federal Law Enforcement Training Center (FLETC), located in Glynco, GA, to create a training program that will help state, local and municipal police officers to identify potential terrorist-related planning activities the officers may encounter in the course of their duties. The pilot training program, which will take place through April 14, will place a special focus on commercial vehicles. The officers will be trained in spotting suspicious driver behavior, identifying fraudulent driver's licenses and counterfeit commercial vehicle documents, and search techniques to locate suspected weapons of mass destruction. The FLETC, a component of the Department of Homeland Security, currently conducts training for federal law enforcement officers and agents from more than 80 agencies. Employing a "train-the-trainer" approach will allow the TSA/FLETC training program to reach enforcement agencies at the federal, state and local levels quickly and effectively. As more officers are trained, TSA and the FLETC will work to ensure that the course of instruction remains current.

Source: http://www.tsa.gov/public/display?theme=44&content=090005198_01c8d5d

[[Return to top](#)]

Postal and Shipping Sector

25. *April 13, Click2Houston (TX)* — **Toy car causes Hazmat scare at post office.** A toy car caused a hazardous materials scare at the Spring post office Wednesday afternoon, KPRC Local 2 reported. The Spring Volunteer Fire Department and Harris County Hazmat team were called to the post office on Spring Cypress at Interstate 45 at about 1:15 p.m. after postal workers complained of eye irritation from a suspicious package. An area of the post office was roped off, but no one was evacuated. Fire officials said fuel in the toy car caused the eye irritation. The postal workers were checked out at the scene and did not need to go to the hospital.

Source: <http://www.click2houston.com/news/8647633/detail.html>

[[Return to top](#)]

Agriculture Sector

26. *April 13, Agriculture Research Service* — **Scientists mobilize fungus to fight hydrilla.** Even the toughest weeds have their mortal enemies. For hydrilla, it's *Mycocleptodiscus terrestris*. Agricultural Research Service (ARS) microbiologist Mark Jackson and U.S. Army Corps of Engineers (USACE) plant pathologist Judy Shearer chose the fungal pathogen for its specificity and cell-wreaking attacks on hydrilla. Originally sold in the 1950s for aquarium use, hydrilla has become a noxious weed of lakes, rivers, canals and other water systems across the southern U.S. and in Atlantic and Pacific coast states. Its dense mats can degrade fish and wildlife habitat. Since 2000, Shearer and Jackson, with ARS' National Center for Agricultural Utilization Research, have collaborated on developing *M. terrestris* for integration with chemical and cultural hydrilla-control strategies. Their efforts led to a patented method of culturing the fungus and "coaxing" it to form tiny, filamentous clumps called microsclerotia. Fortunately, they're just as deadly to hydrilla. When dusted onto potted hydrilla in aquarium trials, the microsclerotia reduced plants' above-ground growth by 99 percent.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

27. *April 10, Rochester Democrat and Chronicle (NY)* — **Area farm wages expanding war on potato worm.** Larry and Joe Guilian's Livingston, NY, farm is infested with an invasive species, a rare strain of root-eating microscopic worm known to exist on just one other farm in the entire U.S. New York's entire multimillion-dollar produce industry will be at risk if the worm cannot be contained to the satisfaction of the Canadian government. If the worm begins to spread, the border could be closed to a wide range of crops. The villain in the story is the golden nematode. Nematodes are typically introduced as hard brown cysts in the soil. Once their target prey — plants such as potatoes, tomatoes and eggplants — begins to grow, the eggs within these cysts sense a chemical signal indicating that roots are developing. They hatch and start feeding on these roots. Infested plants rarely die, but they're of little use to farmers. Sated, the female nematodes burrow into the roots. Once they're fertilized by the free-crawling males, they swell into amber-colored spheres the size of a pinhead, each filled with eggs. Undisturbed, the process repeats itself over and over again until the soil is teeming with millions of nematodes.

Golden nematode information:

<http://www.aphis.usda.gov/ppq/ispm/nematode/background.html>

Source: <http://www.democratandchronicle.com/apps/pbcs.dll/article?AID=20060410/NEWS01/604100335/1002/NEWS>

[[Return to top](#)]

Food Sector

28. *April 05, U.S. Food Safety and Inspection Service* — **Ham salad recalled.** Town and Country Meats, a Greene, ME, firm, is voluntarily recalling approximately 92 pounds of ham salad that

may be contaminated with *Listeria monocytogenes*, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) April 5. The ham salad was produced on March 31 and April 3, 2006, and was distributed to retail establishments in Maine. The problem was discovered through company microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. Consumption of food contaminated with *Listeria monocytogenes* can cause listeriosis, an uncommon but potentially fatal disease. Healthy people rarely contract listeriosis.

Source: http://www.fsis.usda.gov/News_&_Events/RECALL_012_2006_RELEA_SE/index.asp

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

29. *April 13, Agence France–Presse* — Bird flu confirmed in third Afghan province. The H5N1 strain of bird flu deadly to humans has been confirmed in a third province in Afghanistan. Tests in Italy confirmed that H5N1 was found in birds in the central province of Logar, the Food and Agriculture Organization said. The strain has also been found in Kabul and in eastern Nangarhar province on the border with Pakistan. No human cases of the disease have been reported in the country. About 85 percent of the Afghan population live in close contact with poultry, officials have said.

Source: http://news.yahoo.com/s/afp/20060413/hl_afp/healthfluafghani stan_060413095616

30. *April 12, Associated Press* — Air travel involved in mumps epidemic spread. Two infected airline passengers may have helped spread Iowa's mumps epidemic to six other Midwestern states, health officials said Wednesday, April 12. "These people may have exposed other people on those planes or in these airports," said Kevin Teale, a spokesperson for the Iowa Department of Public Health. The mumps epidemic is the nation's first in 20 years. Health officials say 515 suspected cases have been reported in Iowa, and the disease also has been seen in six neighboring states, according to the U.S. Centers for Disease Control and Prevention. As of Monday, April 10, Nebraska had 43 reported cases; Kansas, 33; Illinois, four; Missouri, four; Wisconsin, four; and Minnesota, one. The Iowa health department identified two people who were potentially infectious when they were traveling in late March and early April.

Mumps information: http://www.cdc.gov/ncidod/diseases/submenus/sub_mumps.htm

Source: http://hosted.ap.org/dynamic/stories/M/MUMPS_IN_THE_AIR?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2006-04-12-16-39-19

31. *April 12, Imperial College* — Novel virus entry mechanism could lead to new drugs against poxviruses. An Imperial College research team discovered the mechanism allowing Vaccinia virus to shed its outer lipid membrane and enter cells. The mechanism is unique in virology and paves the way for development of new antiviral drugs. Many viruses are surrounded by a single lipid membrane, or envelope, and to enter cells this membrane must be removed. Previously, all

enveloped viruses were thought to shed their lipid membrane by fusion with a cell membrane which allows the virus core to be released into the cell. In contrast, the extracellular form of Vaccinia virus has two lipid membranes, meaning a single fusion event will not release a naked virus core into the cell. The researchers found that interactions between polyanionic or negatively charged molecules on the cell surface and glycoproteins on the virus particle caused a non-fusogenic disruption of the virus outer envelope, allowing the poxvirus to enter the cell. As well as discovering how the double membrane problem is solved, the researchers demonstrated that polyionic compounds can be used to treat poxvirus infections, even days after infection has started. Disrupting the outer membrane with polyanionic compounds exposes the virus, allowing antiviral antibodies to be more effective.

Source: <http://www.imperial.ac.uk/P7693.htm>

32. *April 12, Agence France–Presse* — **New cases of H5N1 found in Russian province.** The H5N1 strain of the bird flu virus has been found among dozens of dead hens in Russia's southern region of Volgograd, in the second such case in two weeks, an official with the local administration said. Samples were sent to the city of Vladimir, east of Moscow, where the type of virus was to be more thoroughly tested, the official said. Twenty-five hens died Tuesday, April 11, in the village of Kolobrodovo, in the Frolovo district of the Volgograd region. The village was placed under quarantine. H5N1 had already been found among dozens of dead birds in the Volgograd region late last month. Russia's chief veterinarian Sergei Dankvert warned last month that bird flu was posing a growing threat to the country.

Source: http://news.yahoo.com/s/afp/20060412/hl_afp/healthflurussia_060412195502;_ylt=AsKVe.sOoKnLgCdh4ROVe6qJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

33. *April 12, University of California–Berkeley* — **Yeast may cut cost of malaria drug.** Researchers striving to create a less expensive version of the antimalarial drug, artemisinin, have cleared a major hurdle. Two and a half years ago, a University of California–Berkeley, team led by Jay Keasling, professor of chemical engineering and bioengineering, succeeded in engineering bacteria to make a chemical precursor of artemisinin — the best drug available to cure malaria. The team's ultimate goal was to retool the microbe's metabolism to perform as much of the drug synthesis as possible in order to sidestep the expensive laboratory synthesis needed to make artemisinin. That synthesis would have increased the drug's cost beyond the researchers' ambitious target of 25 cents per dose. They now have nearly achieved that goal by engineering the production of artemisinic acid, one chemical alteration away from artemisinin. The fact that the researchers have not yet been able to produce artemisinin itself is not a disadvantage, they said, since drugs currently on the market — all made from extracts of the wormwood plant, *Artemisia annua* — are synthetic derivatives of both artemisinic acid and artemisinin.

Source: http://www.berkeley.edu/news/media/releases/2006/04/12_malaria.shtml

[[Return to top](#)]

Government Sector

Nothing to report.

[[Return to top](#)]

Emergency Services Sector

34. *April 13, Houston Chronicle* — **Five hurricane drills planned for the Gulf Coast.** The Department of Homeland Security will organize five regional hurricane exercises along the Gulf Coast to assess what states and local communities might need from the federal government if another catastrophic hurricane strikes this year, Secretary Michael Chertoff said Wednesday, April 12. Chertoff announced plans for the hurricane drills over the next 60 days, during a speech to more than 2,000 emergency management officials attending the National Hurricane Conference this week. The upcoming drills will force government at all levels to "test and retest improvements made to hurricane plans, to identify efforts where we might have to redouble our efforts by June 1," said Chertoff said, referring to the opening of hurricane season.
Chertoff's remarks at the National Hurricane Conference:
<http://www.dhs.gov/dhspublic/display?content=5533>
Source: <http://www.chron.com/dispatch/story.mpl/nation/3790885.html>
35. *April 13, Richmond Times–Dispatch* — **Two million dollars distributed to 25 areas in Virginia to improve interoperability.** Firefighters and rescue workers in Hanover County, VA, will be able to radio their counterparts in Richmond and other neighbors in a regional emergency. Police in Petersburg will be able to monitor video feeds from a safe distance and retrieve medical data from hospitals. Hanover and Petersburg are two of the 25 Virginia localities that learned Thursday, April 13, that they will receive federal grants in the next two weeks to improve the ability of emergency communications systems to talk to one another in a disaster. Virginia is distributing \$2 million through its homeland security grant program.
Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMSGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1137835339860&path=!news&s=1045855934842
36. *April 12, Portsmouth Herald (NH)* — **Communication a concern in nuke plant drill.** An earthquake hit a mile offshore near Seabrook Station nuclear power plant in Seabrook, NH, Tuesday, April 11 — as part of an emergency response drill. Federal Emergency Management Agency evaluators on site took notes of what went right and wrong. The main problem in the town of Seabrook appeared to be the lag time in communication between the state's Incident Field Office in Newington and the town's emergency operations center at the fire station. Seabrook officials said, in a real emergency, they would have begun evacuations long before receiving the go-ahead from the state. The delay in communication is due to the chain of calls and because the drill is squeezed into a few hours, said Jim van Dongen, spokesperson for the state Office of Emergency Management.
Source: <http://www.seacoastonline.com/news/04122006/news/97251.htm>
37. *April 12, Kodiak Daily Mirror (AK)* — **Report finds 'kinks' in Alaska's emergency response preparedness.** A recently released report gives Kodiak, AK, good marks for its mock drill held in March for emergency preparedness in case of a community terrorism attack or natural disaster. Emergency crews came out in force March 14 in response to a simulated explosion of tanks storing diesel at North Pacific Fuel near Pier 2. The evaluation report of the March drill stated communications with the hospital were "problematic," largely due to poor reception of

hand-held radios within the building. Also, communications with the Emergency Operations Center proved difficult. The report pointed out that medevacs to and from the hospital may be needed in the future. Some confusion was also found with the handling of media and public information.

Source: <http://www.kodiakdailymirror.com/?pid=19&id=2954>

38. *April 12, U.S. Department of Homeland Security* — **FEMA releases New Orleans advisory flood data.** Federal Coordinator for Gulf Coast Rebuilding Donald Powell, U.S. Army Corps of Engineers Commander Lt. Gen. Carl Strock, Federal Emergency Management Agency (FEMA) Director of Mitigation and Administrator of the National Flood Insurance Program David Maurstad, and FEMA Deputy Director for Gulf Coast Recovery Gil Jamieson Tuesday, April 12, announced the release of advisory flood data for New Orleans and the majority of the surrounding area. The flood advisories will inform residents how to reduce or mitigate flood risks as they begin reconstruction, and will provide guidance to communities for better and stronger rebuilding. They also announced the release of U.S. Army Corps of Engineers revised estimates of costs to certify and further enhance the area's levees. Powell announced that the Administration plans to begin working with Congress immediately to address additional funding beyond what the Administration has already requested, estimated at \$2.5 billion, for work in all of the New Orleans area, except for lower Plaquemines. Those improvements will provide 100-year protection to about 98 percent of the population in the New Orleans area.
- Source: <http://www.dhs.gov/dhspublic/display?content=5531>

39. *April 12, Kodiak Daily Mirror (AK)* — **Alaska officials attend bird flu summit.** A team of key players from Kodiak, AK, were in Anchorage Thursday, April 13, attending a statewide summit on preparations for an outbreak of pandemic flu. The governor's office called the group together as part of an interagency effort to address a possible epidemic in Alaska. After the meeting, the Kodiak team brought back information on how to put together local safeguards to protect the community. The aim of statewide planning is to bring state and local governments together to battle a pandemic if one should occur.
- Source: <http://www.kodiakdailymirror.com/?pid=19&id=2952>

[[Return to top](#)]

Information Technology and Telecommunications Sector

40. *April 13, ZDNET (Australia)* — **Boot Camp security risk is just hype: Gartner.** Any talk of Apple's Boot Camp software exposing the company's operating system to security risks is just hype and should be ignored, according to analyst firm Gartner. In a Garner advisory, research vice-president Michael Silver said: "The Mac software will be located on another partition within a different file system; thus, running Windows on a Mac will not expose the Mac software to more malware." However, if Boot Camp helps to increase the penetration of Apple's platform then OS X could attract the attention of cyber-criminals, he said.
- Source: http://www.zdnet.com.au/news/software/soa/Boot_Camp_security_risk_is_just_hype_Gartner/0,2000061733,39251707,00.htm

41. *April 12, Security Focus* — **Sun Solaris sh(1) local denial-of-service vulnerability.** Sun

Solaris Bourne shell sh(1) is prone to a local denial-of-service vulnerability. Analysis: A security vulnerability in the Bourne shell may allow an unprivileged local user to cause sh(1) processes to crash while creating temporary files. This can lead to a denial-of-service for scripts or for users (such as 'root') that use sh(1). Vulnerable: Sun Solaris 10.0 _x86; Sun Solaris 10.0; Sun Solaris 9.0 _x86; Sun Solaris 9.0; Sun Solaris 8.0 _x86; Sun Solaris 8.0. Solution: Sun has released an advisory and fixes to address this issue. For more information: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-102 282-1>
Source: <http://www.securityfocus.com/bid/17478/discuss>

42. April 12, Tech Web — Microsoft sparks backlash by tying IE changes to patch. By packaging a functionality change for Internet Explorer (IE) with a needed security update, Microsoft has alienated some IT professionals, security vendors complained Wednesday, April 12. Along with the 10 patches within the Tuesday, April 11, MS06-013 Security Bulletin, Microsoft bundled changes to IE's handling of ActiveX controls. Those changes, which were prompted by a 2003 \$521 million judgment against Microsoft in a patent lawsuit brought by Eolas Technologies Inc. and the University of California, will require users to manually activate controls on some sites. The inclusion of the ActiveX changes "makes everything a mess" for companies deploying and testing Microsoft's monthly patches, said Mike Murray, director of research at vulnerability management vendor, nCircleMurray. Instead, Microsoft should have separated the IE ActiveX changes from the security fixes. "They easily could have deployed it as a separate patch or rolled it into a service pack," said Murray.
Source: <http://www.securitypipeline.com/news/185300871>

43. April 12, Tech Web — Microsoft to pull plug on Windows 98 and Millennium in July. Microsoft has begun reminding users of Windows 98, Windows 98 SE, and Windows Millennium that it will cut off all support for the aging operating systems in July. "Microsoft is ending support for these products because they are outdated and these older operating systems can expose customers to security risks," the company said in a notice posted to its Website. After July 11, Microsoft will no longer provide security updates for them.
Source: <http://www.techweb.com/wire/software/185300689>

44. April 12, Tech Web — Microsoft updates Malicious Software Tool to include three new pieces of malware. Along with the usual patches unveiled Tuesday, April 11, Microsoft also updated the Windows Malicious Software Tool, a free utility that detects and deletes a limited number of worms, viruses, Trojans, and rootkits. April's edition adds three new pieces of malware to the tool's target list: the Valla virus, and Reagle and Locky worms. Microsoft tagged all three as "moderate" threats.
Source: <http://www.techweb.com/wire/security/185300927;jsessionid=IMOE5PQBG2TZQQSND BECKICCCJUM EKJVN>

45. April 11, LURHQ — Report: DNS Cache Poisoning — The Next Generation. The old problem of DNS cache poisoning has again reared its ugly head. While some would argue that the domain name system protocol is inherently vulnerable to this style of attack due to the weakness of 16-bit transaction IDs, the immediate threat cannot be ignored while waiting for something better to come along. There are new attacks, which make DNS cache poisoning trivial to execute against a large number of name servers running today. The LURHQ Threat Intelligence Group has released the report, "DNS Cache Poisoning — The Next Generation," in

order to shed light on these new attacks and recommend ways to defend against them. Refer to the source for the full report.

Source: <http://www.lurhq.com/cachepoisoning.html>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of an active exploitation of a vulnerability in the way Microsoft Internet Explorer handles certain DHTML methods. By persuading a user to access a specially crafted webpage, a remote, unauthenticated attacker may be able to execute arbitrary code on that user's system, or cause Internet Explorer to stop functioning.

For more information please see US-CERT Vulnerability Note:

VU#876678 – Microsoft Internet Explorer createTextRange() vulnerability.

<http://www.kb.cert.org/vuls/id/876678>

Known attack vectors for this vulnerability require that Active Scripting is enabled in Internet Explorer. Disabling Active Scripting will reduce the chances of exploitation.

US-CERT recommends the following:

Apply the appropriate updates, patches, or fixes as prescribed in the Microsoft Security Bulletin MS06-013. Please see URL:

<http://www.microsoft.com/technet/security/Bulletin/MS06-013.msp>

Disable Active Scripting as specified in the Securing Your Web Browser document.

http://www.us-cert.gov/reading_room/securing_browser/#how_to_secure

Read and send email in plaintext format and don't follow unknown web page links.

Review the additional workarounds in the Microsoft Security Advisory 917077.

<http://www.microsoft.com/technet/security/advisory/917077.mspx>

Review Microsoft's recommendations to improve the safety of browsing and email activity. http://www.microsoft.com/athome/security/online/browsing_safety.msp

Phishing Scams

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. US-CERT encourages users to report phishing incidents based on the

following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 32459 (---), 113 (auth), 1027 (icq), 135 (epmap), 139 (netbios-ssn), 445 (microsoft-ds), 25 (smtp), 1434 (ms-sql-m), 6346 (gnutella-svc) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.